AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computer implemented method for tracking changes to a customer system in a managed hosting environment, the method comprising:

detecting predetermined audit intervals to perform periodic audits;

performing the periodic audits of the customer system in accordance with the predetermined audit intervals, the performing of the periodic audits includes executing an agent program that is resident on the customer system and that collects audit data to be transferred to an application server connected with the customer system via a network; and

transferring the audit data to the application server, the application server to perform a comparison of the audit data with previous audit data to detect changes to the customer system;~~,~~ and

correlating the audit data and a set of rules with previous failures and previous security attacks to develop change patterns, wherein the change patterns are used to predict one or more of the following: future failures and future security attacks~~create future audit data based on results of the comparison of the audit data with the previous audit data, wherein the creating of the future audit data is to facilitate future troubleshooting of the customer system~~.

2. (Previously Presented) The method of claim 1, wherein the performing of the periodic audits comprises storing the changes on a database server connected with the application server via the network.

3. (Previously Presented) The method of claim 2, wherein the audit data comprises operating system files, file system, registry, and application software files of the customer system.

4. (Previously Presented) The method of claim 2, wherein the changes are compressed and encrypted prior to being stored.

5. (Previously Presented) The method of claim 1, further comprising:

checking out the customer system from the application server to allow the application server to make the changes to software of the customer system;

suspending the periodic audits;

taking a first snapshot of the customer system;

checking in the customer system when the changes to the software of the customer system have been completed;

taking a second snapshot of the customer system;

generating change data on the application server by comparing the first snapshot and the second snapshot;

storing the change data on the database server; and

resuming the periodic audits.

6. (Previously Presented) The method of claim 5, wherein the first and second snapshots comprise operating system files, file system, registry, and application software files of the customer system.

7. (Previously Presented) The method of claim 5, wherein the change data is compressed and encrypted prior to being stored.

8. (Currently Amended) The method of claim 2, further comprising:

reading ~~a~~ the set of rules from the database server;

applying the set of rules to the change data to determine whether any of the set of rules has been violated; and

responsive to a violation of any of the set of rules, taking an action associated with a rule violated.

9. (Previously Presented) The method of claim 8, wherein the rules are stored on the database server.

10. (Currently Amended) A system, comprising:

a customer system available to a customer in a managed hosting server, the customer system having an agent program to detect a predetermined audit intervals to perform periodic audits, to perform the periodic audits, and to collect audit data to be transferred to an application server;

the application server connected with the customer system via a network to perform a comparison of the audit data with previous audit data to detect changes to the customer system~~, and create future audit data based on results of the comparison of the audit data with the previous audit data, wherein the creating of the future audit data is to facilitate future troubleshooting of the customer system~~;

a database server connected with the application server via the network to store changes detected by the application server, wherein the database server includes a rules engine, the rules engine to correlate the audit data and a set of rules with previous failures and previous security attacks to develop change patterns, wherein the change patterns are used to predict one or more of the following: future failures and future security attacks;

a report server connected with the database server via the network to generate reports based on the changes stored on the database server; and

a command center connected with the application server and the report server via the network to retrieve reports from the report server.

11. (Previously Presented) The system of claim 10, wherein customer system is further to executes the agent program to collects snapshot data responsive to a request from the application server.

12. (Previously Presented) The system of claim 10, wherein the application sever is further to:

store the changes on the database server.

13. (Previously Presented) The system of claim 12, wherein the application server compresses and encrypts the changes before storing the changes on the database server.

14. (Previously Presented) The system of claim 10, wherein the application server is further to:

check out the customer system to allow the application server to make the changes to software of the customer system;

suspend the periodic audits;

take a first snapshot of the customer system;

check in the customer system when the changes to the software of the customer system have been completed;

take a second snapshot of the customer system;

generate change data by comparing the first snapshot and the second snapshot;

store the change data on the database server; and

resume the periodic audits.

15. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

detect predetermined audit intervals to perform periodic audits;

perform the periodic audits of the customer system in accordance with the predetermined audit intervals, the performing of the periodic audits includes executing an agent program that is resident on the customer system and that collects audit data to be transferred to an application server connected with the customer server via a network; ~~and~~

transfer the audit data to the application server, the application server to perform a comparison of the audit data with previous audit data to detect changes to the customer system~~;~~, and

correlating the audit data and a set of rules with previous failures and previous security attacks to develop change patterns, wherein the change patterns are used to predict one or more of the following: future failures and future security attacks~~-create future audit data based on results of the comparison of the audit data with the previous audit data, wherein the creating of the future audit data is to facilitate future troubleshooting of the customer system~~.

16. (Previously Presented) The machine-readable medium of claim 15, wherein the performing of the periodic audits comprises storing the changes on a database server connected with the application server via the network.

17. (Previously Presented) The machine-readable medium of claim 16, wherein the audit data comprises operating system files, file system, registry, and application software files of the customer system.

18. (Previously Presented) The machine-readable medium of claim 16, wherein the changes are is compressed and encrypted prior to being stored.

19. (Previously Presented) The machine-readable medium of claim 15, wherein the sets of instructions which, when executed by the machine, further cause the machine to:

check out the customer system from the application server to allow the application server to make the changes to the software of the customer system;

suspend the periodic audits;

take a first snapshot of the customer system;

check in the customer system when the changes to the software of the customer system have been completed;

take a second snapshot of the customer system;

generate change data on the application server by comparing the first snapshot and the second snapshot;

store the change data on the database server; and

resume the periodic audits.

20. (Previously Presented) The machine-readable medium of claim 19, wherein the first and second snapshots comprise operating system files, file system, registry, and application software files of the customer system.

21. (Previously Presented) The machine-readable medium of claim 19, wherein the change data is compressed and encrypted prior to being stored.

22. (Currently Amended) The machine-readable medium of claim 16, wherein the sets of instructions which, when executed by the machine, further cause the machine to:

read ~~a~~ the set of rules from the database server;

apply the set of rules to the change data to determine whether any of the set of rules has been violated; and

responsive to a violation of any of the set of rules, take an action associated with a rule violated.

23. (Previously Presented) The machine-readable medium of claim 22, wherein the rules are stored on the database server.

24. (Currently Amended) An apparatus, comprising:

a customer system available to a customer in a managed hosting server, the customer system having an agent program to detect a predetermined audit intervals to perform periodic audits, to perform the periodic audits, and to collect audit data to be transferred to an application server; ~~and~~

the application server connected with the customer system via a network to perform a comparison of the audit data with previous audit data to detect changes to the customer system~~, and create future audit data based on results of the comparison of the audit data with the previous audit data, wherein the creating of the future audit data is to facilitate future troubleshooting of the customer system~~; and

a rules engine coupled to the application server, the rules engine to correlate the audit data and a set of rules with previous failures and previous security attacks to develop change patterns, wherein the change patterns are used to predict one or more of the following: future failures and future security attacks.

25. (Previously Presented) The apparatus of claim 24, further comprising:

a database server connected with the application server via the network to store changes detected by the application server;

a report server connected with the database server via the network to generate reports based on the changes stored on the database server; and

a command center connected with the application server and the report server via the network to retrieve reports from the report server.

26. (Previously Presented) The apparatus of claim 24, wherein customer system is further to executes the agent program to collects snapshot data responsive to a request from the application server.

27. (Currently Amended) The apparatus of claim 24, wherein the application sever is further to[[:]] store the changes on the database server.

28. (Previously Presented) The apparatus of claim 27, wherein the application server compresses and encrypts the changes before storing the changes on the database server.

29. (Previously Presented) The system of claim 24, wherein the application server is further to:

check out the customer system to allow the application server to make the changes to software of the customer system;

suspend the periodic audits;

take a first snapshot of the customer system;

check in the customer system when the changes to the software of the customer system have been completed;

take a second snapshot of the customer system;

generate change data by comparing the first snapshot and the second snapshot;

store the change data on the database server; and

resume the periodic audits.